



04/04/08 IF AF

PTO/SB/21 (01-08)

Approved for use through 3/31/2008. OMB 0651-0031  
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/796,599
Filing Date	03/09/2004
First Named Inventor	Weishi Feng
Art Unit	2132
Examiner Name	Martinjeriko P. San Juan
Attorney Docket Number	MP0386

Total Number of Pages in This Submission

## ENCLOSURES (check all that apply)

<input checked="" type="checkbox"/> Fee Transmittal Form  <input checked="" type="checkbox"/> Fee Attached  <input type="checkbox"/> Amendment / Reply  <input type="checkbox"/> After Final  <input type="checkbox"/> Affidavits/declaration(s)  <input type="checkbox"/> Extension of Time Request  <input type="checkbox"/> Express Abandonment Request  <input type="checkbox"/> Information Disclosure Statement  <input type="checkbox"/> Certified Copy of Priority Document(s)  <input type="checkbox"/> Response to Missing Parts/ Incomplete Application  <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s)  <input type="checkbox"/> Licensing-related Papers  <input type="checkbox"/> Petition  <input type="checkbox"/> Petition to Convert to a Provisional Application  <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address  <input type="checkbox"/> Terminal Disclaimer  <input type="checkbox"/> Request for Refund  <input type="checkbox"/> CD, Number of CD(s) _____	<input type="checkbox"/> After Allowance Communication to Technology Center (TC)  <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences  <input checked="" type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)  <input type="checkbox"/> Proprietary Information  <input type="checkbox"/> Status Letter  <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below):  <b>Return receipt postcard.</b>
--	--	---

Remarks

The Commissioner is hereby authorized to charge any additional fees that may be required under 37 CFR 1.16 or 1.17 to Deposit Account No. 08-0750.

## SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Harness, Dickey & Pierce, P.L.C.		
Signature			
Printed name	Michael D. Wiggin		
Date	April 3, 2008	Reg. No.	34,754

## CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Maggie Purvis	Express Mail Label No.	EM 184 987 212 US (4/3/2008)
Signature		Date	April 3, 2008

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.  
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

EM 184 987 212 US

# FEE TRANSMITTAL for FY 2008

Effective 2/8/2006. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$ 510

## Complete if Known

Application Number 10/796,599  
 Filing Date 03/09/2004  
 First Named Inventor Weishi Feng  
 Examiner Name Martinjeriko P. San Juan  
 Art Unit 2132  
 Attorney Docket No. MP0386

## METHOD OF PAYMENT (check all that apply)

☐ Check ☒ Credit card ☐ Money ☐ Other ☐ None  
 Order

☒ Deposit Account:

Deposit  
Account  
Number

08-0750

Deposit  
Account  
Name

Harness, Dickey &amp; Pierce, P.L.C.

The Director is authorized to: (check all that apply)

☒ Charge any underpayment ☒ Credit any overpayments  
☐ Charge any additional fee(s) during the pendency of this application  
☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.

## FEE CALCULATION

## 1. BASIC FILING FEE

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1011	310	2011	155	Utility filing fee	
1012	210	2012	105	Design filing fee	
1013	210	2013	105	Plant filing fee	
1014	310	2014	155	Reissue filing fee	
1005	210	2005	105	Provisional filing fee	
SUBTOTAL (1)					(\$ 0

## 2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

Total Claims	Extra Claims	Fee from below	Fee Paid
	0	0	0
Independent Claims	0	0	0
Multiple Dependent		0	0

Large Entity		Small Entity		Fee Description
Fee Code	Fee (\$)	Fee Code	Fee (\$)	
1202	50	2202	25	Claims in excess of 20
1201	210	2201	105	Independent claims in excess of 3
1203	370	2203	185	Multiple dependent claim, if not paid
1204	210	2204	105	** Reissue independent claims over original patent
1205	50	2205	25	** Reissue claims in excess of 20 and over original patent
SUBTOTAL (2)				(\$ 0

\*\*or number previously paid, if greater; For Reissues, see above

## FEE CALCULATION (continued)

## 3. ADDITIONAL FEES

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	
1252	460	2252	230	Extension for reply within second month	
1253	1,050	2253	525	Extension for reply within third month	
1254	1,640	2254	820	Extension for reply within fourth month	
1255	2,230	2255	1,115	Extension for reply within fifth month	
1401	510	2401	255	Notice of Appeal	510
1402	510	2402	255	Filing a brief in support of an appeal	
1403	1,030	2403	515	Request for oral hearing	
1452	510	2452	255	Petition to revive - unavoidable	
1453	1,540	2453	770	Petition to revive - unintentional	
1462	400	1462	400	Petition fee under 37 CFR 1.17(f)	
1463	200	1463	200	Petition fee under 37 CFR 1.17(g)	
1464	130	1464	130	Petition fee under 37 CFR 1.17(h)	
1807	50	1807	50	Processing fee under 37 CFR 1.17 (q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	810	2809	405	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	810	2810	405	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	810	2801	405	Request for Continued Examination (RCE)	

Other fee (specify) \_\_\_\_\_

\*Reduced by Basic Filing Fee Paid SUBTOTAL (3) (\$510

## 4. SEARCH/EXAMINATION FEES

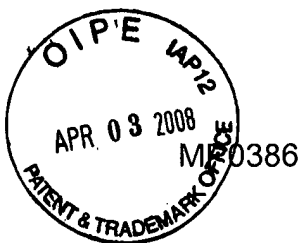
1111	510	2111	255	Utility Search Fee	
1112	100	2112	50	Design Search Fee	
1113	310	2113	155	Plant Search Fee	
1114	510	2114	255	Reissue Search Fee	
1311	210	2311	105	Utility Examination Fee	
1312	130	2312	65	Design Examination Fee	
1313	160	2313	80	Plant Examination Fee	
1314	620	2314	310	Reissue Examination Fee	
SUBTOTAL (4)					(\$0

## SUBMITTED BY

## Complete (if applicable)

Name (Print/Type) Michael D. Wiggins Registration No. (Attorney/Agent) 34,754 Telephone 248-641-1600  
 Signature *Michael D. Wiggins* Date April 3, 2008

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appeal No. \_\_\_\_\_

Application No.: 10/796,599  
Filing Date: March 9, 2004  
Appellant: Weishi Feng  
Group Art Unit: 2132  
Examiner: Martin Jeriko P. San Juan  
Title: SECURE DIGITAL CONTENT DISTRIBUTION SYSTEM  
AND SECURE HARD DRIVE

---

**BRIEF ON APPEAL ON BEHALF OF APPELLANT**

Mail Stop Appeal Brief-Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

April 3, 2008

Sir:

This Appeal is from the decision of the Patent Examiner dated September 14, 2007, rejecting Claims 1-83, which are reproduced in Appendix A of this Appeal Brief.

04/07/2008 HDEMESS1 00000008 10796599

01 FC:1402

510.00 0P

**TABLE OF CONTENTS**

I.	REAL PARTY IN INTEREST .....	3
II.	RELATED APPEALS AND INTERFERENCES .....	3
III.	STATUS OF THE CLAIMS .....	3
IV.	STATUS OF THE AMENDMENTS .....	3
V.	SUMMARY OF THE CLAIMED SUBJECT MATTER .....	4
VI.	GROUND OF REJECTION TO BE REVIEWED ON APPEAL.....	9
VII.	ARGUMENTS .....	9
A.	The Rejections .....	9
B.	Claim Distinctions.....	10
1.	Distinctions regarding independent Claims 1, 20, 31, 50 and 61 .....	10
2.	Dependent Claims 2-19, 21-30, 32-49, 51-60 and 62-83.....	13
VIII.	CONCLUSION .....	17
IX.	APPENDIX A.....	18
	CLAIMS APPENDED .....	18
X.	APPENDIX B.....	36
	EVIDENCE APPENDED .....	36
XI.	APPENDIX C .....	37
	RELATED PROCEEDINGS APPENDED.....	37

**BRIEF ON APPEAL ON BEHALF OF APPELLANT**

In support of the Notice of Appeal filed January 14, 2008, appealing the Examiner's rejection of each of Claims 1-83 in the Final Rejection mailed September 14, 2007, Appellant hereby provides the following remarks.

**I. REAL PARTY IN INTEREST**

The present application is assigned to Marvell International, Ltd. as recorded in the Patent and Trademark Office on March 9, 2004 at Reel 015131, Frame 0782.

**II. RELATED APPEALS AND INTERFERENCES**

The undersigned, the Assignee, and the Appellant does not know of any other appeals or interferences which would directly affect or that would be directly affected by, or have a bearing on, the Board's decision in this Appeal.

**III. STATUS OF THE CLAIMS**

Claims 1-83 are currently pending and are reproduced in the attached Appendix A. Each of these claims is currently pending in the application.

**IV. STATUS OF THE AMENDMENTS**

The claims have not been amended subsequent to the Final Rejection, and there are no unentered amendments.

## **V. SUMMARY OF THE CLAIMED SUBJECT MATTER**

Security of distributed content is important for content providers in preventing piracy. The media that is stored on a disk drive may be separated from the drive, which makes it difficult to defeat bit-by-bit copying of digital content.

The present application in various embodiments relates to secure hard drives (HDs) and systems, as well as methods for distributing digital content. An example of a content distributor is shown in FIG. 2, and an example of a secure HD is shown in FIG. 3A.

The content distributor uses an encryption module to encrypt content that is distributed to the secure HD using a content key. The content key is also encrypted using a public key of the secure HD. The encrypted content and the encrypted content key are downloaded to the secure HD and may be stored on a medium, such as the medium 72 of FIG. 3A.

The secure HD, in order to decrypt the encrypted content, decrypts the encrypted content key. To decrypt the encrypted content key, the secure HD generates a public key and a private key. The public key may be generated using the private key. The private key is generated based on a device specific identification (ID), such as the chip-ID 86 of FIG. 3A. The private key is not stored on the medium or the SOC, rather the private key is generated based on an ID located on the SOC.

The device specific ID is specific to the secure HD and, more particularly, to the system on chip (SOC) of the HD. The device specific ID can not be generated by other devices, such as other HDs that are similar to the secure HD. Thus, should the medium of the secure HD, such as the medium 72, be separated from the secure HD the content thereon cannot be decrypted or copied. Should a hacker that is attempting to decrypt an encrypted content key obtain access to the public key, the hacker would be unable to decrypt the encrypted content key without having the private key (see paragraph [0043] of the present application). This allows distribution of a secure personal content library with a low risk of loss of the digital content to piracy.

Independent Claim 1 recites a secure hard drive that includes a storage medium that stores encrypted digital content and corresponding encrypted content keys (e.g., the HD of FIG. 3A that includes a storage medium 72; and paragraph [0027], lines 1-3). A public key decryption module receives one of the encrypted content keys from the storage medium (e.g., the HD of FIG. 3A that includes a public key decryption module 84 that receives an encrypted content key 64; and paragraph [0028], lines 5-6). The public key decryption module decrypts the encrypted content key using a private key and generates a content key (e.g., the HD of FIG. 3A that includes the public key decryption module 84; paragraph [0028], lines 8-12; and paragraph [0029], lines 1-3). A block decryption module receives the encrypted digital content corresponding to the encrypted content key from the storage medium and the content key from the public key decryption module (e.g., the HD of FIG. 3A that includes a block decryption module 90; and paragraph [0029], lines 1-5). The block decryption module decrypts the encrypted content using the content key (e.g., the HD of FIG. 3A that includes the block decryption module 90; and paragraph [0029], lines 3-5). The private key is generated based on a device specific ID (e.g., the HD of FIG. 3A that includes a chip-ID 86 and the public key decryption module 84 and paragraph [0028], lines 8-11).

Independent Claim 20 recites a secure hard drive that includes a magnetic storage medium and a SOC (e.g., the HD of FIG. 3A that includes the storage medium 72 and SOC 70; and paragraph [0027], lines 1-7). The magnetic storage medium stores encrypted digital content and corresponding encrypted content keys (e.g., the HD of FIG. 3A that includes the storage medium 72; and paragraph [0027], lines 1-3). The SOC includes a public key decryption module and a block decryption module (e.g., the HD of FIG. 3A that includes the SOC 70, the public key decryption module 84 and the block decryption module 90; and paragraphs [0027] and [0029]). The public key decryption module receives one of the encrypted content keys from the magnetic storage medium (e.g., the HD of FIG. 3A that includes a public key decryption module 84 that receives an encrypted content key 64; and paragraph [0028], lines 5-6). The SOC decrypts the encrypted content key using a private key of the SOC to generate a content key (e.g., the HD of FIG. 3A that includes the public key decryption module 84; paragraph [0028], lines 8-12; and paragraph [0029], lines 1-3). The block decryption

module receives the encrypted digital content corresponding to one of said encrypted content keys from the magnetic storage medium and the content key from the public key decryption module (e.g., the HD of FIG. 3A that includes a block decryption module 90; and paragraph [0029], lines 1-5). The block decryption module decrypts the encrypted content using the content key (e.g., the HD of FIG. 3A that includes the block decryption module 90; and paragraph [0029], lines 3-5). The public key decryption module generates the private key based on a device specific ID (e.g., the HD of FIG. 3A that includes a chip-ID 86 and the public key decryption module 84 and paragraph [0028], lines 8-11).

Independent Claim 31 recites a secure hard drive that includes storing means for storing encrypted digital content and corresponding encrypted content keys (e.g., the HD of FIG. 3A that includes a storage medium 72; and paragraph [0027], lines 1-3). Public key decryption means receives one of the encrypted content keys from the storing means (e.g., the HD of FIG. 3A that includes a public key decryption module 84 that receives an encrypted content key 64; and paragraph [0028], lines 5-6). The public key decryption means decrypts the encrypted content key using a private key to generate a content key (e.g., the HD of FIG. 3A that includes the public key decryption module 84; paragraph [0028], lines 8-12; and paragraph [0029], lines 1-3). Block decryption means receives the encrypted digital content corresponding to the encrypted content key from the storing means and the content key from the public key decryption means (e.g., the HD of FIG. 3A that includes a block decryption module 90; and paragraph [0029], lines 1-5). The block decryption means decrypts the encrypted content using the content key (e.g., the HD of FIG. 3A that includes the block decryption module 90; and paragraph [0029], lines 3-5). The private key is generated based on a device specific ID (e.g., the HD of FIG. 3A that includes a chip-ID 86 and the public key decryption module 84 and paragraph [0028], lines 8-11).

Independent Claim 50 recites a secure hard drive that includes magnetic storing means for storing encrypted digital content and corresponding encrypted content keys and a SOC (e.g., the HD of FIG. 3A that includes the storage medium 72 and SOC 70; and paragraph [0027], lines 1-7). The SOC includes public key decryption means for receiving one of the encrypted content keys from the magnetic storage means (e.g., the



HD of FIG. 3A that includes a public key decryption module 84 that receives an encrypted content key 64; and paragraph [0028], lines 5-6). The SOC decrypts the encrypted content key using a private key of the SOC to generate a content key (e.g., the HD of FIG. 3A that includes the public key decryption module 84; paragraph [0028], lines 8-12; and paragraph [0029], lines 1-3). Block decryption means receives the encrypted digital content corresponding to the encrypted content key from the magnetic storing means and the content key from the public key decryption means (e.g., the HD of FIG. 3A that includes a block decryption module 90; and paragraph [0029], lines 1-5). The block decryption means decrypts the encrypted content using the content key (e.g., the HD of FIG. 3A that includes the block decryption module 90; and paragraph [0029], lines 3-5). The public key decryption module generates the private key based on a device specific ID (e.g., the HD of FIG. 3A that includes a chip-ID 86 and the public key decryption module 84 and paragraph [0028], lines 8-11).

Independent Claim 61 recites a method for distributing digital content that includes storing encrypted digital content and corresponding encrypted content keys on a storage medium (e.g., the HD of FIG. 3A that includes a storage medium 72; and paragraph [0027], lines 1-3). One of the encrypted content keys is received from the storage medium (e.g., the HD of FIG. 3A that includes a public key decryption module 84 that receives an encrypted content key 64; and paragraph [0028], lines 5-6). The encrypted content key is decrypted using a private key to generate a content key (e.g., the HD of FIG. 3A that includes the public key decryption module 84; paragraph [0028], lines 8-12; and paragraph [0029], lines 1-3). The encrypted digital content corresponding to the encrypted content key is received from the storage medium (e.g., the HD of FIG. 3A that includes a block decryption module 90; and paragraph [0029], lines 1-5). The encrypted content is decrypted using the content key (e.g., the HD of FIG. 3A that includes the block decryption module 90; and paragraph [0029], lines 3-5). The private key is generated based on a device specific ID (e.g., the HD of FIG. 3A that includes a chip-ID 86 and the public key decryption module 84 and paragraph [0028], lines 8-11).

Dependent Claim 10 recites the secure hard drive of Claim 9 and requires that the public key decryption module perform digital signature verification of a content

directory entry corresponding to content that is selected for play (e.g., paragraph [0032]; paragraph [0034], lines 1-3; paragraph [0038], lines 1-3; paragraph [0040], lines 5-6; and paragraph [0042], lines 1-7).

Dependent Claim 11 recites the secure hard drive of Claim 9 and requires that a content directory entry contain a clear content counter that specifies a portion of a corresponding content that is not encrypted (e.g., paragraph [0036], lines 7-10 and paragraph [0041]).

Dependent Claim 27 recites the secure hard drive of Claim 26 and requires that the public key decryption module performs digital signature verification of a content directory entry corresponding to content that is selected for play (e.g., paragraph [0032]; paragraph [0034], lines 1-3; paragraph [0038], lines 1-3; paragraph [0040], lines 5-6; and paragraph [0042], lines 1-7).

Dependent Claim 40 recites the secure hard drive of Claim 39 and requires that the public key decryption means performs digital signature verification of the content directory entry corresponding to the content that is selected for play (e.g., paragraph [0032]; paragraph [0034], lines 1-3; paragraph [0038], lines 1-3; paragraph [0040], lines 5-6; and paragraph [0042], lines 1-7).

Dependent Claim 41 recites the secure hard drive of Claim 39 and requires that a content directory entry contain clear content counting means for specifying a portion of the corresponding content that is not encrypted (e.g., paragraph [0036], lines 7-10 and paragraph [0041]).

Dependent Claim 57 recites the secure hard drive of Claim 56 and requires that the public key decryption means performs digital signature verification of a content directory entry corresponding to content that is selected for play (e.g., paragraph [0032]; paragraph [0034], lines 1-3; paragraph [0038], lines 1-3; paragraph [0040], lines 5-6; and paragraph [0042], lines 1-7).

Dependent Claim 67 recites the method of Claim 66 and further includes performing digital signature verification of the content directory entry corresponding to the content that is selected for play (e.g., paragraph [0032]; paragraph [0034], lines 1-3; paragraph [0038], lines 1-3; paragraph [0040], lines 5-6; and paragraph [0042], lines 1-7).

Dependent Claim 79 recites the secure hard drive of claim 78 and requires that the device specific ID is an ID associated with the secure hard drive (e.g., the HD of FIG. 3A that includes a chip-ID 86; and paragraph [0028], lines 8-11).

Dependent Claim 83 recites the secure hard drive of claim 1 and requires that the public key decryption module generates the private key based on a chip ID of the secure hard drive (e.g., the HD of FIG. 3A that includes a chip-ID 86; and paragraph [0028], lines 8-11).

## **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Appellant seeks the Board's review of the rejection of Claims 1-21, 23-79 and 81-83 under 35 U.S.C. 103(a) as being unpatentable over Sims III (U.S. Pat. No. 6,550,011; hereinafter "Sims") in view of Tai et al. (U.S. Pub. No. 2004/0034785; hereinafter "Tai").

## **VII. ARGUMENTS**

### **A. The Rejections**

The rejections that are the subject of this Appeal are the rejections of each of independent Claims 1, 20, 31, 50 and 61 and dependent Claims 10, 11, 27, 40, 41, 57, 67, 79 and 83 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Sims in view of Tai.

With respect to independent Claims 1, 20, 31, 50 and 61, the Examiner alleges that Sims discloses a public key decryption module that receives an encrypted content key from a storage medium and that decrypts the encrypted content key using a private key to generate a content key. See page 3 of the Final Office Action of September 14, 2007.

The Examiner admits that Sims fails to disclose the generation of the private key, which is used to decrypt the encrypted content key, using a device specific ID. In an

attempt to make up for the admitted deficiency of Sims, the Examiner notes that Tai teaches an encrypted mechanism that uses a chip die ID to generate a private key (referring to paragraph [0037] of Tai; see Page 4, Lines 1-4 of the Final Office Action).

With respect to dependent Claims 10, 27, 40, 57 and 67, the Examiner alleges that Sims discloses a public key decryption module that performs digital signature verification of a content directory entry corresponding to content that is selected for play and refers to col. 15, line 48 and to col. 17, line 25 of Sims.

With respect to dependent Claims 11 and 41, the Examiner alleges that Sims discloses where a content directory entry contains a clear content counter that specifies a portion that is not encrypted and refers to col. 15, lines 7-21 and to col. 11, lines 34-46 of Sims.

With respect to dependent Claims 79 and 83, the Examiner alleges that a chip ID is intrinsic to the device where the chip is being utilized.

## **B. Claim Distinctions**

### **1. Distinctions regarding independent Claims 1, 20, 31, 50 and 61**

Appellant respectfully submits that Sims and Tai fail to show, teach, or suggest all of the limitations of Appellant's Claims 1, 20, 31, 50 and 61.

With respect to Claims 1, 20, 31, 50 and 61, Sims and Tai fail to at least show, teach, or suggest a secure hard drive public key decryption module that decrypts an encrypted content key using a private key that is generated based on a device specific ID. Note that the private key is not used to decrypt encrypted content, but rather is used to provide a content key for such decryption. Sims and Tai fail to show, teach or suggest the stated decryption.

As Claims 1, 20, 31, 50 and 61 recite a public key decryption module for a HD that encrypts a content key, Claims 1, 20, 31, 50 and 61 are directed to distributed

content. In a distributed content environment, the content is encrypted by a distributor prior to reception by end users. The end users decrypt the content based on a received content key and a public/private key combination.

Traditionally, hard drives that are similar to each other may have or have access to the same private/public key sets. Thus, for example, should a storage medium such as a disk (platter) be removed from a hard drive, another hard drive may be able to decrypt information on that disk. The invention of Claim 1 prevents such access and limits decryption of content on a disk to only an individual hard drive with the device specific ID.

The Examiner admits that Sims fails to disclose a private key that is generated based on a device specific ID. For at least this reason, Sims also fails to disclose decryption of an encrypted content key using a private key that is generated via a device specific ID.

The Examiner alleges that Tai discloses a private key that is generated via a device specific ID. The Examiner further alleges that the keys of Sims and Tai are cryptographic keys and because of this it would have been obvious to generate the device specific key of Sims using the private key generation technique of Tai. Appellant submits that the private key of Tai is substantially different and is used differently than the device secret key of Sims and the private key of Claim 1.

As best understood by Appellant, Sims is directed to security of distributed content. The device secret key of Sims is used to decrypt a content key, which is in turn used to decrypt distributed content.

In contrast and as best understood by Appellant, Tai is directed to security of boot-up software that is transferred between memories of a device. Tai discloses a private key that is used to encrypt boot-up software of a device, not to decrypt a content key. The boot-up software is locally stored on the device and is not distributed. The device includes ROM and a controller with RAM. The boot-up software is stored in the ROM. Upon an initial power up of the controller at an end product manufacturing site, the boot-up software is downloaded from the ROM to the RAM. The controller encrypts the boot-up software using a 64-bit number that is based on a chip's die ID number.

Once encrypted, the boot-up software is up-loaded and stored on the ROM for future use.

The boot-up software of Tai is encrypted at the manufacturing site and stored on the ROM prior to the corresponding computer system being delivered to an end user. Once the end user receives the computer system, the encrypted software is simply decrypted for use by the computer system. Thus, this encryption of Tai is directed to boot-up software that is stored and that remains on an onboard memory of a device. Tai is not directed to content that is distributed over a network. Tai does not use content keys and/or private/public key combinations.

In paragraph [0053], Tai states that previously known solutions use public and private keys, whereas the system of Tai creates an encryption key by itself. Tai states that public and private keys are not used. Thus, Tai explicitly teaches away from the use of public/private key combinations. Therefore, Tai does not disclose the decryption of an encrypted content key using a private key that is generated via a device specific ID.

Since there is no operative relationship between the device secret key of Sims and the private key of Tai and since Tai teaches away from the use of public/private key combinations, there would be no reason to combine and/or modify the decryption techniques of Sims using the private key encryption of Tai. In Sims, the content key is distributed to multiple end users and the device secret key is used to decrypt a content key, not to encrypt distributed content. In Tai, the boot-up software is locally and internally encrypted via the private key. The boot-up software is not used for the decryption of a content key. Also, throughout Tai it is stated that private and public keys are not used, see paragraphs [0011] and [0053] and claim 3 of Tai. Thus, the protection techniques and applications of Sims and Tai are substantially different.

Also, Applicant further submits that cryptography is a very broad area. Cryptography is used in various mathematic, computer science, and engineering applications. The mere suggestion that the references can be combined based on the references being in the field of cryptography falls far short of the **explicit analysis** that is required by the Supreme Court in *KSR Int'l v. Teleflex Inc.*, 550 U.S. \_\_\_\_ (2007). Absent such an express teaching or suggestion in the references, the explicit analysis

and reasoning must be supplied by the Examiner. *Id.* In other words, the Examiner is required to provide explicit reasoning as to why one skilled in the art would be motivated to decrypt a content key using a private key that is generated based on a device specific ID. Here, the Examiner merely notes that it would have been obvious to generate the device specific key of Sims using the private key generation technique of Tai and fails to provide explicit analysis and reasoning as required.

In addition, when a reference teaches away from the claimed subject matter, a rejection based on obviousness can not stand. See *In re Sullivan*, 498 F.3d 1345 (Fed. Cir. Aug. 29, 2007). Evidence rebutting a prima facie case of obviousness can include "that the prior art teaches away from the claimed invention in any material respect", *Id.* As Claim 1 is directed to distributed content and recites use of a content key, a public/private key combination is inherently used. Explicit use of a public key is recited at least in dependent Claims 22 and 80.

Furthermore, one cannot simply replace the device secret key of Sims with the private key of Tai, as the keys are used differently. The private key of Tai is used for encryption of boot-up software and the device secret key of Sims is used for the decryption of an encrypted content key. Thus, it is improper to combine the teachings of Sims and Tai, as suggested.

It is a longstanding rule that to establish a prima facie case of obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 180 USPQ 143 (CCPA 1974), see M.P.E.P. §2143.03.

Therefore, Claims 1, 20, 31, 50 and 61 should be allowable for at least the above reasons.

## **2. Dependent Claims 2-19, 21-30, 32-49, 51-60 and 62-83**

Claims 2-19, 21-30, 32-49, 51-60 and 62-83 ultimately depend from Claims 1, 20, 31, 50 and 61 and should be allowable for at least similar reasons.

With respect to Claims 10, 27, 40, 57 and 67, the Examiner alleges that Sims and Tai disclose a public key decryption module that performs digital signature verification of a content directory entry corresponding to content that is selected for play,

as claimed. The Examiner refers to col. 15, line 48 and to col. 17, line 25 of Sims for such disclosure.

In col. 15, lines 46-49, Sims discloses encryption of content use information in order to protect the information from unauthorized alterations. In col. 17, lines 23-27, Sims discloses the comparing of a public key to content use information to determine if a device is authorized to receive content. These sections do not disclose signature verification of a content directory corresponding to content that is selected for play. Applicant is unable to find disclosure of this feature anywhere in Sims.

In the Advisory Action of December 7, 2007, the Examiner further states that Sims discloses the use of a public key and digital certificates that teach the use of digital signatures to verify if a device is authorized to receive content based on content use information. Appellant submits that this is irrelevant, as the verification by a distributor that a receiving device is authorized to receive content, is unrelated to a public key decryption module of a receiving device that performs digital signature verification.

In Sims a distributor confirms that a user device or device that is receiving distributed content is authorized prior to transmission of the content. In contrast, the claimed secure HD, which may be referred to as a device that receives distributed content, performs a digital signature verification. Also, the secure HD performs this verification on a content directory entry corresponding to content that is selected for play. This feature is simply not provided in the relied upon art.

Thus, Claims 10, 27, 40, 57 and 67 are further allowable for at least the above reasons.

With respect to Claims 11 and 41, the Examiner alleges that Sims and Tai disclose a content directory entry that contains a clear content counter that specifies a portion of a corresponding content that is not encrypted, as claimed. The Examiner refers to col. 15, lines 7-21 of Sims for such disclosure.

In the Advisory Action, the Examiner states that the clear content counter is used to track content that is permitted to be played. Appellant submits that the clear content counter is not only directed to content that is permitted to be played, but also to distributed content that is not encrypted.



The claimed clear content counter is used to indicate a portion of digital content that is received from a distributor that is not encrypted. The clear content counter refers to content that is received by a distributor, that is identified as inactive by the distributor, but is not encrypted and thus can be played. When content is inactive, a receiving device is normally unable to play the content, as the content is encrypted and/or protected by a digital signature of the content distributor. However, a distributor may provide a sample of inactive content. The sample is received from the distributor and may be unencrypted, allowing a receiver to play the corresponding content. See paragraphs [0032] and [0041] of the present application.

In col. 15, lines 7-21, Sims discloses content use information that includes rules establishing authorized use of content. The rules include a permitted number of playback times and indication of when content should be deleted. In other words, Sims discloses content use information that includes the number of playback iterations permitted and when content should be removed from a user's device. The content use information is unrelated to what content is encrypted. Knowledge of a number of permitted playbacks and when content should be deleted also does not suggest what portion of content is active. The content use information appears to be applied to content that is active in its entirety.

The Examiner further refers to col. 11, lines 34-46 of Sims for the disclosure of the limitations of Claims 11 and 41. In col. 11, lines 34-46, as best understood by Appellant, Sims discloses a generation counter and other content use information. The generation counter is used to count movement of a content key. See col. 15, lines 11-13 of Sims. The generation counter is unrelated to unencrypted content. The other content use information mentioned in col. 11, lines 34-46 does not include a counter.

Thus, Claims 11 and 41 are further allowable for at least the above reasons.

With respect to Claims 79 and 83, Sims and Tai do not at least show, teach or suggest a device specific ID that is an ID associated with a secure hard drive. The Examiner alleges that a chip ID is intrinsic to a device where the chip is being utilized. Appellant submits that this is irrelevant as a chip ID may be used differently and for a

different purpose. For this reason, systems that operate based on a chip ID may perform different functions and provide a different end result.

Appellant submits that Sims does not disclose the use of a chip ID. Although Tai discloses the use of a chip ID, the use appears to be with respect to a computer or host device, not a hard drive. It appears that the controller of Tai is not a HD or part of a HD. The chip's die ID number is located on a controller of an integrated circuit that has RAM for storage of boot-up software. It appears that the controller of Tai is a controller of a host/computer, not a controller of a HD.

The chip ID of Tai is used for the encryption of boot-up software. The chip ID claimed is used for the decryption of an encrypted content key. The use as explained above by Tai is substantially different than the use recited in the claims of the present application. As the use is substantially different, the system operations with respect to the use of a chip ID are also substantially different.

Thus, Claims 79 and 83 are further allowable for at least the above reasons.

**VIII. CONCLUSION**

Appellant respectfully requests the Honorable Board of Patent Appeals and Interferences to reverse the Examiner's rejection of each of pending Claims 1, 10, 11, 20, 27, 31, 40, 41, 50, 57, 61, 67, 79 and 83. Appellant respectfully submits that the prior art does not teach or suggest one or more limitations of the claims as discussed above. Accordingly, for at least the aforementioned reasons, Appellant respectfully requests the Honorable members of the Board of Patent Appeals and Interferences to reverse the outstanding rejections and objections in connection with the present application and permit each of Claims 1-83 to be passed to allowance in connection with the present application.


Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Michael D. Wiggins, at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By:

  
Michael D. Wiggins  
Reg. No. 34,754

MDW/JJC

**Please address all correspondence to:**

**Harness, Dickey & Pierce, P.L.C.**

**5445 Corporate Drive**

**Suite 200**

**Troy, MI 48098**

**Customer No. 26703**

**Phone. No. (248) 641-1600**

**Fax. No. (248) 641-0270**

**IX. APPENDIX A****CLAIMS APPENDED**

This is a complete and current listing of the claims.

1. A secure hard drive, comprising:
  - a storage medium that stores encrypted digital content and corresponding encrypted content keys;
  - a public key decryption module that receives one of said encrypted content keys from said storage medium and that decrypts said encrypted content key using a private key and generates a content key; and
  - a block decryption module that receives said encrypted digital content corresponding to said one of said encrypted content keys from said storage medium and said content key from said public key decryption module and that decrypts said encrypted content using said content key,wherein said private key is generated based on a device specific identification (ID).
2. The secure hard drive of Claim 1 wherein said storage medium is a magnetic storage medium.
3. The secure hard drive of Claim 1 wherein said public key decryption module and said block decryption module are implemented by a system on chip (SOC).

4. The secure hard drive of Claim 1 further comprising:
  - a content player that receives said decrypted digital content from said block decryption module and that generates at least one of an analog output signal and a digital output signal; and
  - an ID module that provides said device specific ID,
  - wherein said public key decryption module generates said private key using said device specific ID and then generates said content key based on said private key.
5. The secure hard drive of Claim 1 further comprising a controller that performs buffer management and timing of read/write operations.
6. A system comprising the secure hard drive of Claim 5 and further comprising:
  - an external host; and
  - a control interface that provides a communications interface between said controller and said external host.
7. The system of Claim 6 wherein said external host is one of a computer and a portable media player.

8. The secure hard drive of Claim 4 further comprising a watermark detector that communicates with an output of said content player and that determines whether said analog signal that is output by said content player contains a watermark.

9. The secure hard drive of Claim 1 wherein said storage medium stores a content directory having content directory entries for said content.

10. The secure hard drive of Claim 9 wherein said public key decryption module performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

11. The secure hard drive of Claim 9 wherein at least one of said content directory entries contains a clear content counter that specifies a portion of said corresponding content that is not encrypted.

12. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content distributor ID field that identifies a content distributor supplying said corresponding content.

13. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback.

14. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a signature field for said content distributor supplying said corresponding content.

15. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storage medium.

16. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storage medium.

17. The secure hard drive of Claim 1 wherein said content includes at least one of audio, video, and still pictures.

18. The system of Claim 6 further comprising:  
a distributed communications network; and  
a content distributor that transmits encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed communications network.

19. The secure hard drive of Claim 1 wherein said storage medium contains encrypted content that is pre-stored thereon.

20. A secure hard drive, comprising:

- a magnetic storage medium that stores encrypted digital content and corresponding encrypted content keys;
- a system on chip (SOC) including:
  - a public key decryption module that receives one of said encrypted content keys from said magnetic storage medium and that decrypts said encrypted content key using a private key of said SOC to generate a content key; and
  - a block decryption module that receives said encrypted digital content corresponding to said one of said encrypted content keys from said magnetic storage medium and said content key from said public key decryption module and that decrypts said encrypted content using said content key,
- wherein said public key decryption module generates said private key based on a device specific identification (ID).

21. The secure hard drive of Claim 20 further comprising a content player that receives said decrypted digital content from said block decryption module and that generates an analog output signal.



22. The secure hard drive of Claim 20 further comprising a chip ID module that provides said device specific ID for said SOC, wherein said private key and a public key of said SOC are based on said chip ID.

23. The secure hard drive of Claim 20 wherein said SOC further includes a controller that performs buffer management and timing of read/write operations.

24. A system comprising the secure hard drive of Claim 23 and further comprising:

an external host; and

a control interface that provides an interface between said controller and said external host.

25. The secure hard drive of Claim 21 further comprising a watermark detector that communicates with an output of said content player and that determines whether said analog signal that is output by said content player contains a watermark.

26. The secure hard drive of Claim 20 wherein said magnetic storage medium stores a content directory having content directory entries for said content.

27. The secure hard drive of Claim 26 wherein said public key decryption module performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

28. The secure hard drive of Claim 26 wherein at least one of said content directory entries contains at least one of a clear content counter that specifies a portion of said corresponding content that is not encrypted, a content distributor ID field that identifies a content distributor supplying said corresponding content, a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback, a signature field for said content distributor supplying said corresponding content, a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said magnetic storage medium, and a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said magnetic storage medium.

29. The secure hard drive of Claim 20 wherein said content includes at least one of audio, video, and still pictures.

30. The system of Claim 24 further comprising:  
a distributed communications network; and  
a content distributor that transmits encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed communications system.

31. A secure hard drive, comprising:

storing means for storing encrypted digital content and corresponding encrypted content keys;

public key decryption means for receiving one of said encrypted content keys from said storing means and for decrypting said encrypted content key using a private key to generate a content key; and

block decryption means for receiving said encrypted digital content corresponding to said one of said encrypted content keys from said storing means and said content key from said public key decryption means and for decrypting said encrypted content using said content key,

wherein said private key is generated based on a device specific identification (ID).

32. The secure hard drive of Claim 31 wherein said storing means includes a magnetic storing medium.

33. The secure hard drive of Claim 31 wherein said public key decryption means and said block decryption means are implemented by a system on chip (SOC).

34. The secure hard drive of Claim 31 further comprising:

content playing means for receiving said decrypted digital content from said block decryption means and for generating at least one of an analog output signal and a digital output signal; and

an ID means for providing said device specific ID,

wherein said public key decryption means generates said private key using said device specific ID and then generates said content key based on said private key.

35. The secure hard drive of Claim 31 further comprising controller means for performing buffer management and timing of read/write operations.

36. A system comprising the secure hard drive of Claim 35 and further comprising:

an external host; and

control interface means for providing a communications interface between said controller means and said external host.

37. The system of Claim 36 wherein said external host is one of a computer and a portable media player.

38. The secure hard drive of Claim 34 further comprising watermark detecting means that communicates with an output of said content playing means for determining whether said analog signal that is output by said content playing means contains a watermark.

39. The secure hard drive of Claim 31 wherein said storing means stores a content directory having content directory entries for said content.

40. The secure hard drive of Claim 39 wherein said public key decryption means performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

41. The secure hard drive of Claim 39 wherein at least one of said content directory entries contains clear content counting means for specifying a portion of said corresponding content that is not encrypted.

42. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content distributor ID field that identifies a content distributor supplying said corresponding content.

43. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback.

44. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a signature field for said content distributor supplying said corresponding content.

45. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storing means.

46. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storing means.

47. The secure hard drive of Claim 31 wherein said content includes at least one of audio, video, and still pictures.

48. The system of Claim 36 further comprising:  
distributed means for providing a distributed communications network; and  
content distributor means for transmitting encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed means.

49. The secure hard drive of Claim 31 wherein said storing means contains encrypted content that is pre-stored thereon.

50. A secure hard drive, comprising:

magnetic storing means that stores encrypted digital content and corresponding encrypted content keys;

a system on chip (SOC) including:

public key decryption means for receiving one of said encrypted content keys from said magnetic storage means and for decrypting said encrypted content key using a private key of said SOC to generate a content key; and

block decryption means for receiving said encrypted digital content corresponding to said one of said encrypted content keys from said magnetic storing means and said content key from said public key decryption means and for decrypting said encrypted content using said content key,

wherein said public key decryption module generates said private key based on a device specific identification (ID).

51. The secure hard drive of Claim 50 further comprising content playing means for receiving said decrypted digital content from said block decryption means and for generating an analog output signal.

52. The secure hard drive of Claim 50 further comprising chip ID means for providing said device specific ID for said SOC, wherein said private key and a public key of said SOC is based on said chip ID.

53. The secure hard drive of Claim 50 wherein said SOC further includes controller means for performing buffer management and timing of read/write operations.

54. A system comprising the secure hard drive of Claim 53 and further comprising:

an external host; and

control interface means provides an interface between said controller means and said external host.

55. The secure hard drive of Claim 51 further comprising watermark detecting means that communicates with an output of said content playing means for determining whether said analog signal that is output by said content playing means contains a watermark.

56. The secure hard drive of Claim 50 wherein said magnetic storage means stores a content directory having content directory entries for said content.

57. The secure hard drive of Claim 56 wherein said public key decryption means performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

58. The secure hard drive of Claim 56 wherein said content directory entries contain at least one of clear content counting means for specifying a portion of said



corresponding content that is not encrypted, a content distributor ID field that identifies a content distributor supplying said corresponding content, a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback, a signature field for said content distributor supplying said corresponding content, a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said magnetic storing means, and a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said magnetic storing means.

59. The secure hard drive of Claim 50 wherein said content includes at least one of audio, video, and still pictures.

60. The system of Claim 54 further comprising:

distributed means for providing a distributed communications network; and

content distributor means for transmitting encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed means.

61. A method for distributing digital content, comprising:

(a) storing encrypted digital content and corresponding encrypted content keys on a storage medium;

- (b) receiving one of said encrypted content keys from said storage medium;
- (c) decrypting said encrypted content key using a private key to generate a content key;
- (d) receiving said encrypted digital content corresponding to said one of said encrypted content keys from said storage medium;
- (e) decrypting said encrypted content using said content key, and
- (f) generating said private key based on a device specific identification (ID).

62. The method of Claim 61 wherein said storage medium is a magnetic storing medium.

63. The method of Claim 61 further comprising generating at least one of an analog output signal and a digital output signal based on said decrypted digital content.

64. The method of Claim 61 further comprising interfacing with an external host.

65. The method of Claim 63 further comprising determining whether said analog signal contains a watermark.

66. The method of Claim 61 further comprising storing a content directory having content directory entries for said content on said storage medium.

67. The method of Claim 66 further comprising performing digital signature verification of said content directory entry corresponding to said content that is selected for play.

68. The method of Claim 66 further comprising specifying a portion of said corresponding content that is not encrypted using a clean content field in at least one of said content directory.

69. The method of Claim 66 further comprising identifying a content distributor supplying said corresponding content using a content distributor ID field in at least one of said content directory entries.

70. The method of Claim 66 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storage medium.

71. The method of Claim 66 wherein at least one of said content directory entries includes a signature field for said content distributor supplying said corresponding content.

72. The method of Claim 66 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storing means.

73. The method of Claim 66 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storing means.

74. The method of Claim 61 wherein said content includes at least one of audio, video, and still pictures.

75. The method of Claim 64 further comprising:  
providing a distributed communications network; and  
transmitting encrypted content, an encrypted content key, and a content directory entry for a content selection from at least one content distributor to said secure hard drive via said external host and said distributed communications network.

76. The method of Claim 61 further comprising pre-storing encrypted content on said storage medium.

77. The method of Claim 61 further comprising performing steps (b), (c), (d) and (e) using a system on chip (SOC).

78. The secure hard drive of claim 1 wherein said public key decryption module generates said private key based on said device specific ID.

79. The secure hard drive of claim 78 wherein said device specific ID is an ID associated with the secure hard drive.

80. The secure hard drive of claim 78 wherein said public key decryption module generates a public key based on said private key and generates said content key based on said public key.

81. The secure hard drive of claim 1 wherein said public key decryption module generates said private key based on a device specific ID.

82. The secure hard drive of claim 1 wherein said public key decryption module generates said private key based on a chip ID.

83. The secure hard drive of claim 1 wherein said public key decryption module generates said private key based on a chip ID of the secure hard drive.

**X. APPENDIX B**

**NO EVIDENCE APPENDED**

**XI. APPENDIX C**

**NO RELATED PROCEEDINGS APPENDED**